



State Information Technology Advisory Committee (SITAC)

**September 8, 2015
Pioneer Room
State Capitol Building**



Agenda

<u>Time</u>	<u>Topic</u>	<u>Presenter</u>
2:00	Welcome / Opening Comments	Mike Ressler
2:05	Enterprise Architecture Update	Jeff Quast
2:15	2015 Legislative Update	Mike Ressler
2:30	STAGEnet Cybersecurity Discussion	Duane Schell
3:30	Security Updates and ITD Application Hosting Services	Dan Sipes
4:00	Large Project Reporting Overview Health Dept. - NDIIS Job Service - WyCAN Closeout Report	Justin Data Kris Vollmer Cheri Giesen
4:25	Open Discussion / Closing Comments	Mike Ressler



Mike Ressler

CIO





Welcome & Opening Comments



Jeff Quast

**Program
Administrator**

**Enterprise
Architecture**





EA 2.0

- Continue to transition to new EA framework
- All standards have been reviewed and many are actively being updated
- Expecting fewer standards and more guidelines or best practices
- Events now being posted on ITD's public web site, including meeting Recaps
 - Recaps may not include sensitive information



EA Waivers

- Waiver granted to Bank of North Dakota for the Web Domain Name standard
 - RUReadyND.com
 - BND will migrate to a .gov domain by 6/30/17 expiration
- Waiver granted to Game and Fish for the Physical Access standard
 - Mobile devices in vehicles won't screen lock until 45 minutes vs. 15 minutes
 - Contingent on a GNF policy for unattended vehicles being secured and devices being secured in docking stations



Mike Ressler

CIO





2015 Legislative Update

- ITD Received 13 New Positions
- CJIS Program was Transferred over to the AG Budget
- Center for Distance Ed (CDE) Received Strong Support
- 19 Agencies Received Funding for ITD's New Desktop Service
- ITD Received \$1,500,000 for Determining Feasibility of a State Trunked Radio Interoperability Network (Working with State Interoperability Exec Committee)



Duane Schell
Director

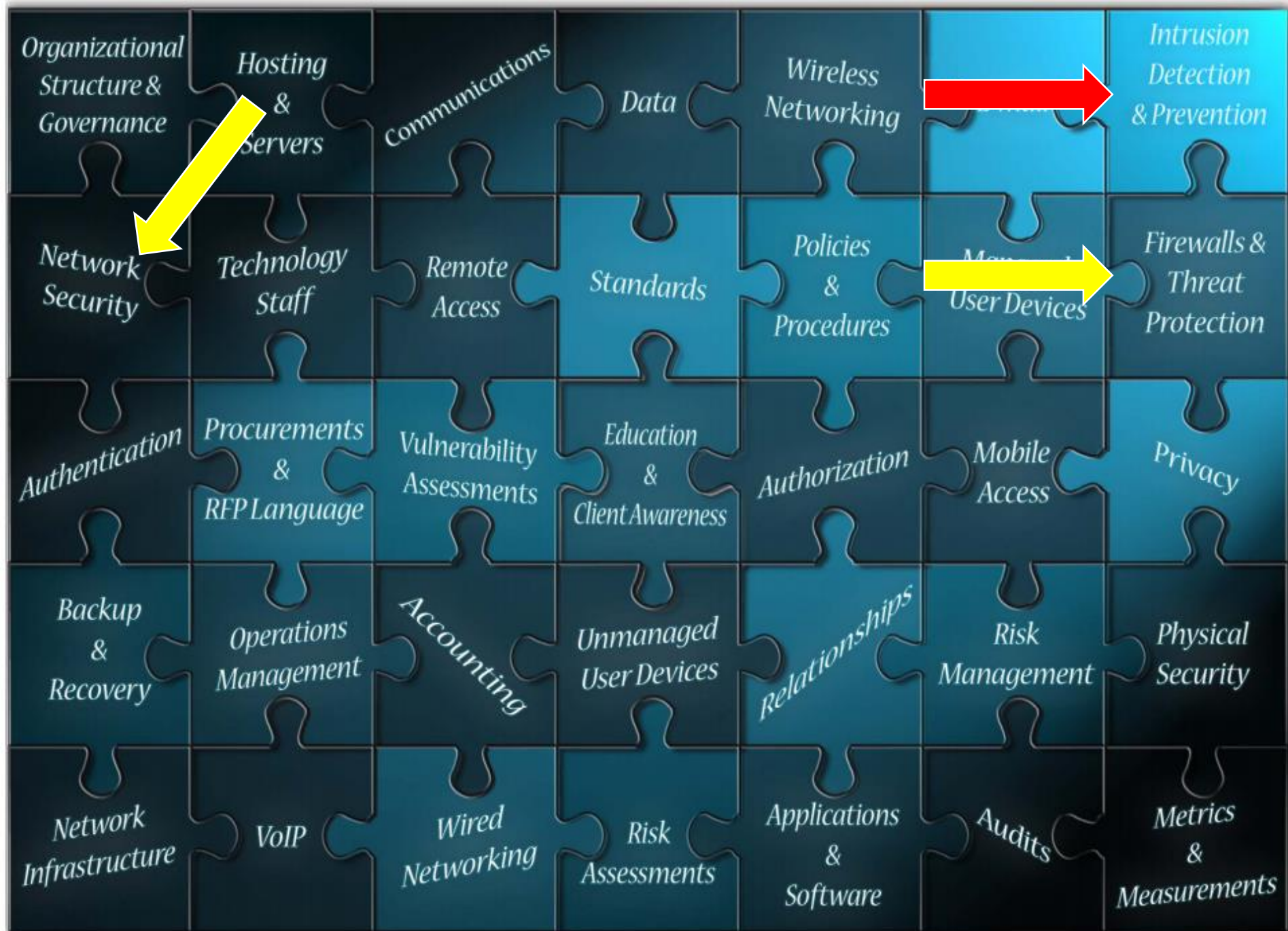
Network Services
Division





Cybersecurity Discussion

- Purpose of today's discussion:
 - Awareness of the volume and types of malicious activity affecting STAGEnet
 - Mitigation efforts that exist at the network layer
 - Implications of those efforts





Intrusion Detection and Prevention

- Intrusion Detection Services -monitors for malicious activity and provides reports
- Intrusion Prevention Services - actively prevents or block malicious activity



Security Boundaries

- Internet
- Data Center
- STAGEnet Customers



Internet

STAGEnet

Data Center



Internet

State

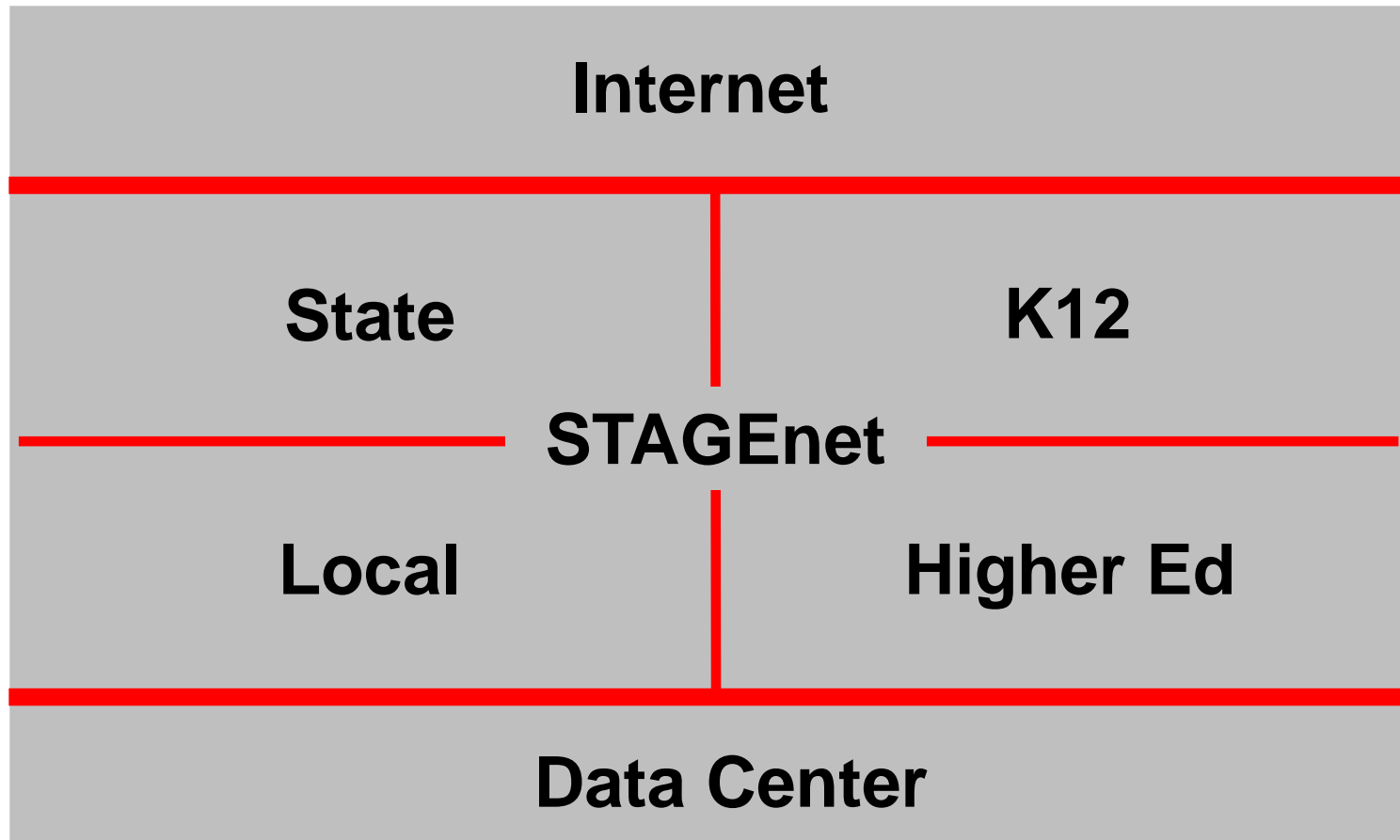
K12

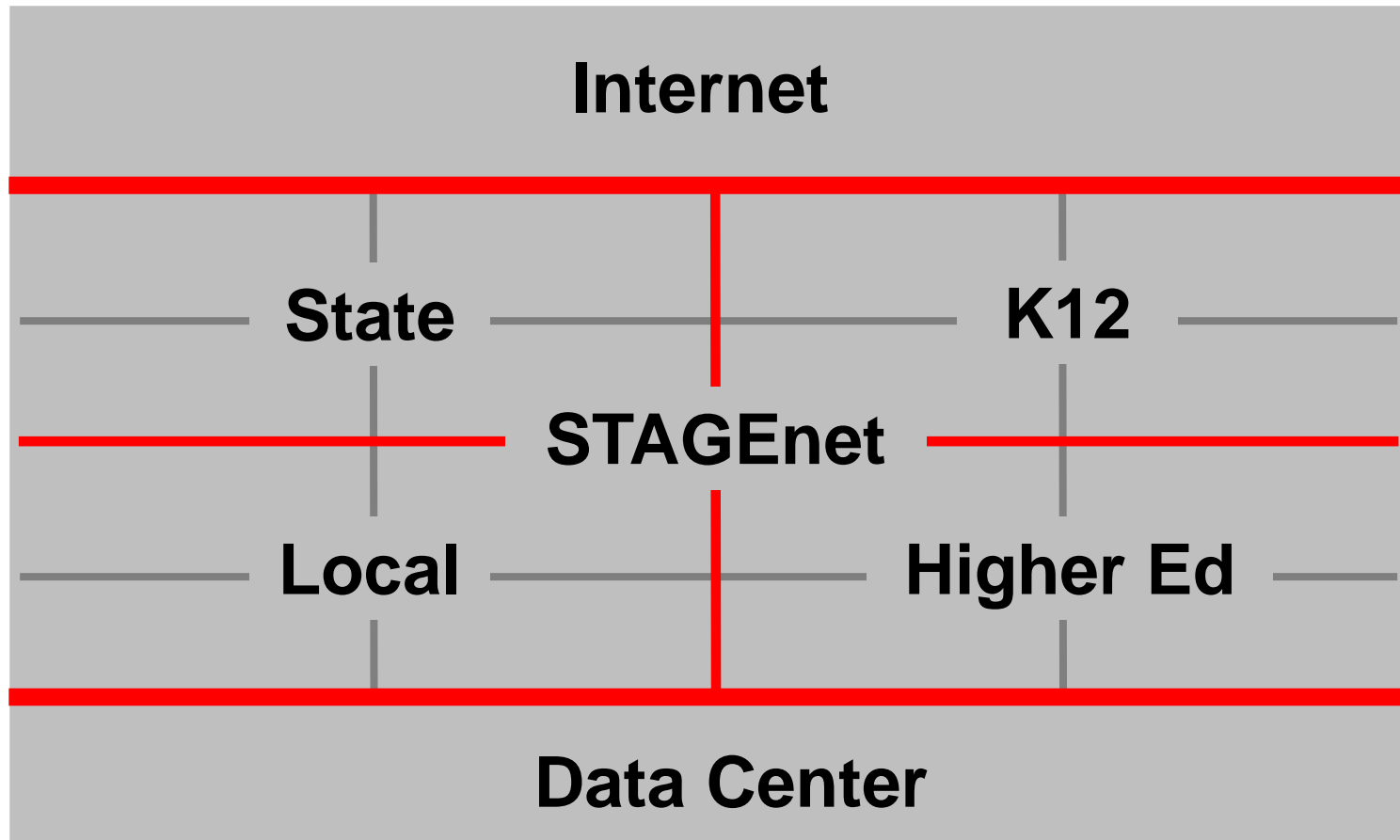
STAGEnet

Local

Higher Ed







Data Center










Type of threats mitigated

Threat Prevention		Types
	Threat/Content Type	Count
1	spyware	1.2 M 
2	scan	41.3 K 
3	virus	16.3 M 
4	flood	616 
5	vulnerability	1.4 M 
6	wildfire-virus	2.3 K 



Scans

Threat Prevention					
	Severity	Threat/Content Name	ID	Threat/Cont... Type	Count
1	MEDIUM	SCAN: Host Sweep	8002	scan	25.7 K 
2	MEDIUM	SCAN: TCP Port Scan	8001	scan	13.0 K 
3	MEDIUM	SCAN: UDP Port Scan	8003	scan	2.6 K 



Vulnerabilities

Threat Prevention

	Severity	Threat/Content Name	ID	Threat/Cont... Type	Count
1	HIGH	MS-RDP Brute-force Attempt	40021	vulnerability	649.0 K
2	HIGH	MAIL: User Login Brute-force Attempt	40007	vulnerability	342.6 K
3	HIGH	Microsoft SQL Server User Authentication Brute-force Attempt	40010	vulnerability	184.8 K
4	HIGH	SSH User Authentication Brute-force Attempt	40015	vulnerability	88.6 K
5	HIGH	Microsoft Windows win.ini access attempt	30851	vulnerability	35.2 K
6	HIGH	HTTP Unauthorized Brute-force Attack	40031	vulnerability	30.7 K
7	CRITICAL	WordPress Login BruteForce Attempt	40044	vulnerability	28.8 K
8	CRITICAL	Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Vulnerability	32735	vulnerability	24.2 K
9	HIGH	Generic HTTP Cross Site Scripting Attempt	31477	vulnerability	16.2 K
10	CRITICAL	Bash Remote Code Execution Vulnerability	36729	vulnerability	8.8 K



Spyware




Threat Prevention

	Severity	Threat/Content Name	ID	Threat/Cont... Type	Count
1	LOW	Sipvicious.Gen User-Agent Traffic	13272	spyware	810.3 K
2	CRITICAL	ZeroAccess.Gen Command and Control Traffic	13235	spyware	343.1 K
3	MEDIUM	Suspicious DNS Query (generic:F15vfB9.upasinfection.ru)	4037030	spyware	8.4 K
4	CRITICAL	salicy.Gen Command And Control Traffic	14468	spyware	4.2 K
5	MEDIUM	Suspicious DNS Query (generic:mwujqiknxkeiya.cc)	4026110	spyware	3.5 K
6	CRITICAL	Suspicious.Gen Command And Control Traffic	14155	spyware	2.6 K
7	MEDIUM	Suspicious DNS Query (generic:w5ELjEJtC.upasspreads.ru)	4037079	spyware	1.4 K
8	MEDIUM	Suspicious DNS Query (generic:utggames-poker.com)	4032080	spyware	1.1 K
9	MEDIUM	Suspicious DNS Query (generic:ectstorage.softlayer.net)	4035465	spyware	1.0 K
10	MEDIUM	generic:aqyq8uar0g6h.mxp2141.com	3839934	spyware	984



Flood (DDOS)

Threat Prevention

	Severity	Threat/Content Name	ID	Threat/Cont... Type	Count
1	CRITICAL	ICMP Flood	8503	flood	323 
2	CRITICAL	UDP Flood	8502	flood	276 
3	CRITICAL	TCP Flood	8501	flood	22 



Virus

Threat Prevention

	Severity	Threat/Content Name	ID	Threat/Cont... Type	Count
1	MEDIUM	Virus/Win32.WGeneric.fyodg	2557362	virus	16.2 M
2	MEDIUM	Virus/Win32.WGeneric.dgoou	2686801	virus	1.9 K
3	MEDIUM	Virus/Win32.WGeneric.fxgwl	2263940	virus	734
4	MEDIUM	Virus/Win32.WGeneric.gapht	2192411	virus	646
5	MEDIUM	Virus/Win32.wplug.cbq	2453106	virus	415
6	MEDIUM	Virus/Win32.WGeneric.fxsqf	2894861	virus	395
7	MEDIUM	Trojan/Win32.upatre.bcti	2279769	virus	197
8	MEDIUM	Virus/Win32.ba.cde	1203858	virus	166
9	MEDIUM	Virus/Win32.dloadr.ivr	1210136	virus	136
10	MEDIUM	Trojan/Win32.upatre.bcei	2750020	virus	96



Network based virus detection

- Benefits
 - Catch virus before it reaches user device
 - Detect and mitigation zero day “new” viruses
- Weakness
 - Does not catch viruses from other sources
 - USB drives or Other networks
- Complimentary to client based AV protections



Source of threats?

- [Example Worldwide Threat Map](#)



North Dakota Information Technology Department





Ongoing Effort

- Threat landscape is evolving
 - Ongoing tuning effort
 - Leverage Partner
 - Vendors
 - MS-ISAC
 - NASTD
 - NASCIO
 - False positives can and do occur



Not all protection is the same

- User population
 - Large and diverse community
- Data Center
 - Contains critical assets
 - Contains clearly identifiable assets
 - Allows for very fine grain and strong controls



Closing

- Threat is real, significant and evolving
- Mitigation efforts at the Network Layer exist and generate value
- Committed to improving and evolving the overall security posture of STAGEnet



Dan Sipes Deputy CIO





Security Updates

- SOC2 Audit - http://www.nd.gov/auditor/reports/i112_15.pdf
- Multi-Factor Authentication for Privileged Accounts
- Managed Security Services - MS-ISAC
- Cybersecurity Roles and Responsibilities
- Web Server Cyber Attack



Cybersecurity Roles and Responsibilities

- Six Main Roles and Responsibilities
 - Senior Management (ITD)
 - Information Security Management (ITD)
- Information Owner (State Agencies)
 - Agency Director
 - Agency IT Coordinator
 - Agency Security Officer
- Technology Providers (ITD or Vendors)
- Supporting Functions (Audit, Physical Security, DR)
- Users (State Agencies and their Stakeholders)



Cybersecurity Roles and Responsibilities

- ITD's Role (IS Security Management and Technology Provider)
 - Per NDCC 54-59-05.2 and 54-59-05.14 ITD has the authority and responsibility for information systems security surrounding State of North Dakota information technology assets.
 - ITD is responsible for protecting the availability, integrity, and confidentiality of the state's information systems and the data stored in information systems that are managed by ITD.
 - ITD also directs the development of standards, policies and guidelines for enterprise security. This is done in collaboration with state agencies through the Enterprise Architecture process.



Cybersecurity Roles and Responsibilities

- Information Owner (State Agencies)
 - ITD does not own most of the information residing in the data center. The information owner for most data is a state agency or political subdivision.
 - The information owner is responsible for authorizing access privileges and ensuring regular reviews and updates to manage changes in risk profiles.



Cybersecurity Roles and Responsibilities

- Agency Director
 - Agency Directors are responsible for information security in each agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise.
 - The director also is responsible for ensuring compliance with state enterprise security policies and with state and federal regulations.
 - Per NDCC 54-59-10 each agency must appoint an information technology coordinator to maintain a liaison with ITD. The agency director will often delegate their information security responsibilities to the agency information technology coordinator.



Cybersecurity Roles and Responsibilities

- **Agency IT Coordinator**
This role is assigned by the Agency Director and their security responsibilities include:
 - Submitting security requests
 - Reviewing access logs
 - Reviewing authorization reports
 - Serving as the main point of contact between ITD and the agency regarding security issues
- These duties are sometimes delegated to the Agency Security Officer.



Cybersecurity Roles and Responsibilities

- Agency Security Officer
 - Agency Security Officers are responsible for communicating with ITD's Security Incident Response Team and coordinating agency actions in response to an information security incident.
 - In many agencies the Agency IT Coordinator fills this role.
- Agency User
 - Responsible for complying with the provisions of IT security policies and procedures.



Web Server Cyber Attack

- Lessons Learned
 - Properly securing and patching third party applications
 - ITD plans to implement more restrictions on the tools agencies and their vendors use to administer web sites.
- Application Inventory and Categorization
 - ITD will be reaching out to agencies to complete an initial application inventory and categorization exercise.
 - Integrates with the Application Portfolio Management role that is part of ITD's Cloud Broker role.
- Scanning critical applications for vulnerabilities
 - Agencies need to budget for this security analysis.



Application Portfolio Management and Cloud Services

- ITD will partner with agencies to manage their application portfolio.
- ITD will serve in a “Cloud Broker” role as agencies evaluate cloud services to meet business needs.
- Aligned with ITD’s hosting responsibilities in NDCC 54-59-22.
- Software as a Service (SaaS) solutions hosted in the cloud require a waiver from OMB and ITD.
- ITD will partner with agencies to manage any on-going contract/relationship with a SaaS vendor.



Application Portfolio Management and Cloud Services

- Application inventory for both on-premise and SaaS applications.
- ITD has a matrix to help assess and categorize the risk associated with applications.
- Assessment Areas
 - IT Architecture/Vendor Capability
 - Identity
 - Security
 - Data
 - Strategic Impact
 - Cost



Application Portfolio Management and Cloud Services

- Contract Management - negotiations and key terms and conditions
 - Cost drivers
 - Escalation caps
 - Hosting location
- Vendor Management
 - Periodic architecture reviews
 - Certification reviews
 - Prior approval of material changes to the cloud architecture environment



Application Portfolio Management and Cloud Services

- Statewide Inventory of Applications
 - Includes on-premise and cloud based solutions
 - Helps to manage overall enterprise risk
 - Helps to ensure consistent contract terms
- Documentation of Integration Points
 - Identify key integration points to the state infrastructure (e.g. Active Directory)
 - Promote common standards based integration where possible



Application Portfolio Management and Cloud Services

- On-premise solutions vs. cloud based solutions
 - Near-term, on premise solutions will be preferred to maintain economies of scale in the data center and allow the state to mature its cloud posture.
- Costs
 - Reviewing current and future rate structures to cover the costs for these activities and infrastructure investments.
 - On-premise solutions embed the costs in existing rates.
 - Cloud based solutions will incur a monthly add-on fee to vendor fees.
 - Applied to new approved cloud waivers starting this biennium.
 - Legacy cloud waivers - no later than 7/1/2017.



Justin Data

ITD Project Management

Large Project Reporting





What does the law say?

2. During the life of the project, the agency shall notify the state information technology advisory committee if:

- a. At a project milestone, the amount expended on project costs exceeds the planned budget for that milestone by twenty percent or more; or

- b. At a project milestone, the project schedule extends beyond the planned schedule to attain that milestone by twenty percent or more.



How do we measure the 20 percent?

- Variance: A measure of performance on a project through an indicated report date
- When planning has been completed, a baseline is set
- Variance is then measured against that baseline
- All major projects use the same “variance spreadsheet”
- *If a baseline becomes completely unworkable a new one may be set based upon a recovery strategy*
- *Projects that do not recover may need to also present at the Legislative I.T. Committee*



Kris Vollmer

ITD Project Management

Health Dept ~ NDIIS





Casual Factors

Key contributors to the project delays & schedule variance:

- NDIIS users unable to access system
- THOR provider portal outages impact NDIIS
- Project schedule variance
- Project resources
- Reporting work & cost effort spent



Lessons Learned

- Understanding new ITD Project Management expectations and reporting requires increased collaboration between ITD & NMIC
- Need continued cross training of NMIC resources
- Need better planning of NMIC technology upgrades to minimize impact to NDIIS deliverables
- Need to enhance system monitoring and communications related to the NDIIS hosted solution



Recovery Strategy

- Assign new NMIC project manager
- Reprioritize and baseline the project deliverables in partnership with DoH
- Gain understanding of the State's Project Management schedule variance calculations
- Evaluate and implement further segregation of the NDIIS environment to increase system stability
 - Strengthen monitoring and upgrade processes
- Commitment to improving collaboration

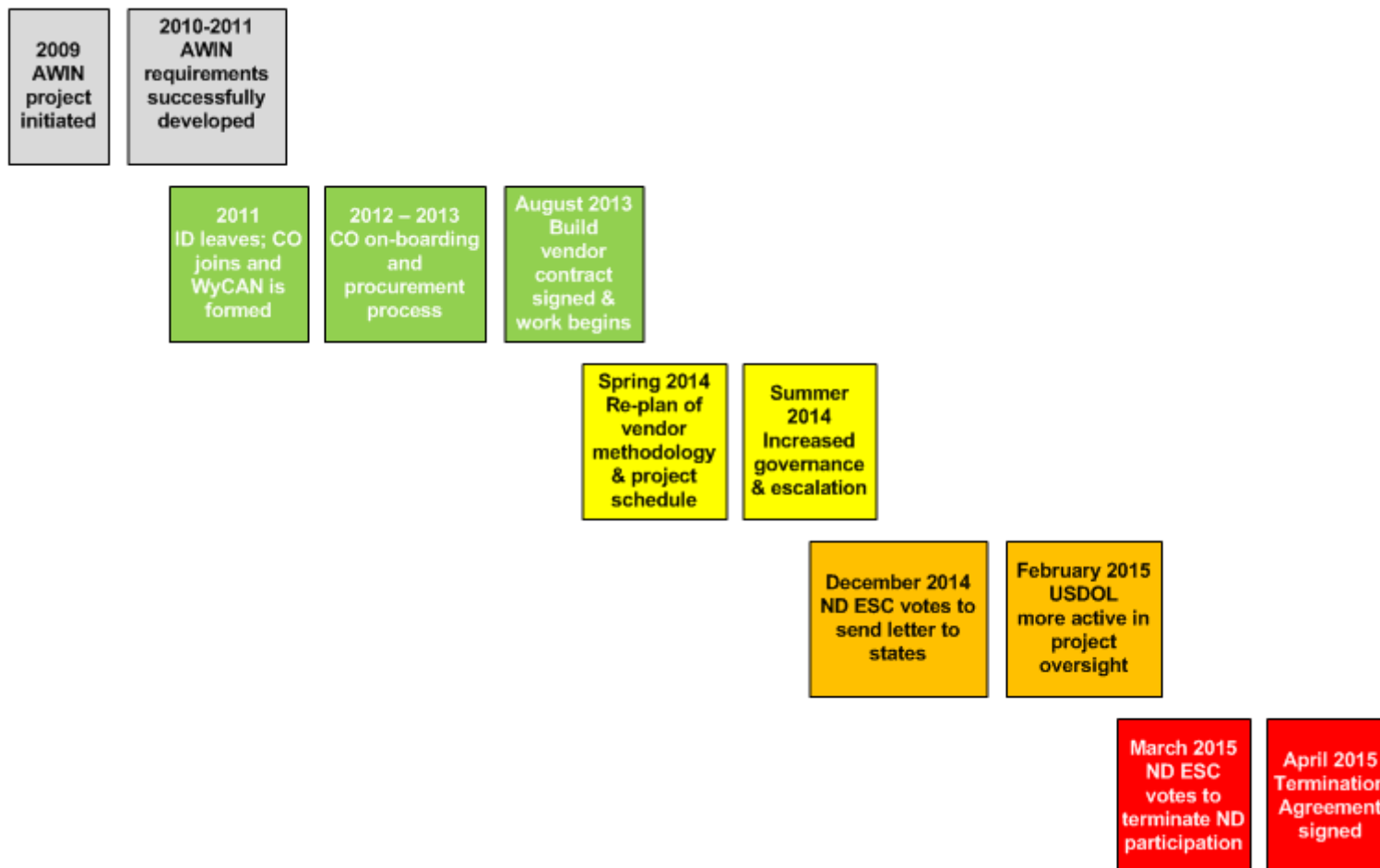


**Cheri Giesen
Executive Director
Job Service North Dakota

WyCAN Close-Out Report**



North Dakota Information Technology Department





Causal Factors

- 1) System being developed no longer aligned with ND's specific needs

Note: No state funds were used on the project.



Lessons Learned

- 1) During a procurement process to obtain a COTS solution, end-users should get significant hands-on experience with the proposed product as opposed to merely receiving a short vendor demonstration.
- 2) Look for a product that is already working in production.
- 3) Strict requirements eliminate vendors.



Best Practices

- 1) Before engaging a vendor, do as much prep work as possible.
- 2) Have well-defined requirements.
- 3) Continually evaluate the alignment of the requirements and objectives against the project and product.
- 4) Use sound project management and governance processes.



Recovery Strategy

- 1) Interim solution
- 2) Exploring other options for long-term
- 3) Take advantage of knowledge gained and JSND work products produced as part of the project



Mike Ressler

CIO





Open Discussion / Closing Comments



THANK YOU!!!